REMARKS/ARGUMENTS

These remarks are made in response to the Office Action of August 7, 2008 (Office Action). As this response is timely filed within the 3-month shortened statutory period, no fee is believed due. However, the Examiner is expressly authorized to charge any deficiencies to Deposit Account No. 50-0951.

Claims Rejections – 35 USC § 103

Claims 1-4 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent 6,988,075 to Hacker, *et al.* (hereinafter Hacker) in view of non-patent literature, "Public Standards and Patients' Control: How to Keep Electronic Medical Records Accessible but Private," BMJ, Feb. 2001; 322, pages 283-287 to Mandl, *et al.* (hereinafter Mandl). Claims 16-18 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Hacker in view of Mandl, and further in view of U.S. Published Patent Application 2002/0010679 to Felsher (hereinafter Felsher).

Applicants respectfully disagree with the rejections and thus have not amended the claims. Applicants have cancelled Claims 5-16 and 19. However, Applicants are not conceding that the cancelled claims fail to present patentable subject matter. The cancellations are solely for the purpose of expediting prosecution. Accordingly, cancellations should not be interpreted as the surrender of any subject matter, and Applicants expressly reserve the right to present the original version of any of the cancelled claims in any future divisional or continuation applications from the present application.

Aspects of Applicants' Invention

It may be helpful to reiterate certain aspects recited in the claims prior to addressing the cited references. One aspect of the invention, as typified by amended Claim 1, is a method of permitting controlled access to medical information of a patient.

The method can include establishing a storage means for storing the medical

information of the patient; establishing a means for accessing the medical information by the patient or any other authorized user; controlling an authorization and a scope of access to the medical information by the patient according to a role of a user accessing the medical information by modifying an access control list. The access control list, more particularly, can list all authorized users and their respective roles.

The method also can include assigning each user with a unique ID and pin, and tracking and notifying the patient of an identity of an entity that accessed the medical information, information that was accessed by the entity, and when the entity accessed the information.

See, e.g., Specification, paragraphs [0008], [0023], and [0035].

The Claims Define Over The Prior Art

Hacker teaches a barcode or card to identify a patient, not a provider or user. The pass phrase suggested by Hacker does not suggest anything unique to the provider, but instead is a code used in conjunction with the patient bar code or card to access a patient sensitive information. Therefore, Hacker does not disclose assigning each user with a unique ID and pin as recited in Claim 1 of the instant application.

It was stated in the Office Action that Hacker does not teach controlling an authorization and a scope of access to the medical information by the patient according to an assigned role of a user accessing the medical information by modifying an access control list, wherein the access control list lists each authorized user and the assigned role of each authorized user. However, it was asserted that these limitations are disclosed by Mandl (see Mandl: page 284, section Confidentiality).

Mandl mentions that the patient can limit the information to specific providers and provides an override mechanism that is controlled by a patient. However, Mandl does not suggest using an access control list as the mechanism for controlling access. Mandl also concedes that their proposed system would likely be compromised based on their

limited confidence in their privacy mechanism (column 1, last paragraph on page 285).

Regarding Claim 3, Hacker suggests the use of a bar code or patient ID card, but does not teach a universally unique identifier. Rather, Hacker teaches an identifier that could be specific only to a particular record system, such as in current hospital systems; the same patient wrist codes (MRN, or Account) may refer to different patients at different hospitals.

Regarding Claim 4, Hacker proposes an override for emergency situations but does not teach the mechanism of registration of emergency providers that would prevent the access to information by those searching for private information and posing to be an emergency provider.

Felsher describes a trustee model for the collection and maintenance and distribution of entrusted information content with an emphasis on the security of the entrusted data using data encryption techniques. While Felsher mentions in paragraph [0189] that the patient has a right to control the release of the records, Felsher focuses on the concept of the virtual trust and how encryption can be used to build that trust.

Regarding Claim 17, this is a key feature in a typical doctors office visit, where computers are provided in each of the patient examining rooms for the direct access and recording of patient private information. When the doctor moves to another room the access to patient information needs to be protected from other patients who might seize the opportunity to browse another's private information. The mechanism of logging into another examining room should immediately prevent access from a prior terminal.

Regarding the Examiner's comments in the first paragraph on page 6 of the Office Action, it is noted that Hacker does not teach the identification or means of identification of an individual accessing private information, and therefore would be unable to provide an accounting as such.

Accordingly, the cited references, alone or in combination, fail to disclose or suggest each and every element of Claim 1. Applicants therefore respectfully submit that Claim 1 defines over the prior art. Furthermore, as each of the remaining claims depends from Claim 1 while reciting additional features, Applicants further respectfully submit that the remaining claims likewise define over the prior art.

Applicants thus respectfully request that the claim rejections under 35 U.S.C. § 103 be withdrawn.

CONCLUSION

Applicants believe that this application is now in full condition for allowance, which action is respectfully requested. Applicants request that the Examiner call the undersigned if clarification is needed on any matter within this Amendment, or if the Examiner believes a telephone interview would expedite the prosecution of the subject application to completion.

Respectfully submitted,

AKERMAN SENTERFITT

Date: September 18, 2008

/Gregory A. Nelson/
Gregory A. Nelson, Registration No. 30,577
Yonghong Chen, Registration No. 56,150
Customer No. 40987
Post Office Box 3188
West Palm Beach, FL 33402-3188
Telephone: (561) 653-5000